Digital Forensics in the Cloud: Research Perspectives.

Professor Jill Slay AM

Polytechnic of Namibia/University of South Australia

Major work

- I am a researcher in forensic computing carrying out research aimed to develop a sound theoretical and scientific foundation for the discipline, based on principles broadly gained from software engineering.

Overview

- ICT and Crime
- Trends in ICT and Crime
- Defining the Field of Digital Forensics
- Development of High Quality Digital Forensics
- Effect of Accreditation on Digital Forensic Process
- Current Forensic Environment in Other Disciplines
- Enter the Cloud!
- Cloud Service and Deployment Models
- E-Crime and Cloud Computing
- Possible Effect of Cloud based Cyber crime
- Recognised Risks (AGIMO)
- State of the Art in Research

ICT and Crime

- Information and communication technology (ICT) has long been used for illegal purposes.
- Techniques have been developed to establish whether an ICT system has been compromised or whether it has been used to store illegal data and files (e.g. child abuse materials for commercial purposes and terrorism-related materials) or as a platform for other crime.
    - There is a constant need for law enforcement and national security agencies to adapt and augment technical and procedural digital forensic responses as criminals, organised crime groups and politically-motivated actors, who are often early adopters, use new technologies in different illegal ways.

Trends in ICT and Crime

- For example, a 2009 study on online child exploitation by the Australian Institute of Criminology pointed out
  - *Better-educated criminals are likely to explore alternatives to hiding data over the internet. These include storing data on password-protected file-sharing websites, email accounts and less reputable content providers hosted in countries with lax cybercrime legislation.*

Defining the Field of Digital Forensics

- Constant need to define and redefine Forensic Computing (or Digital or Network Forensics)
- NOT THE SAME AS LETTING YOUR SYS ADMIN STAFF 'LOOK FOR EVIDENCE'
- McKemmish: *identification, preservation, analysis and presentation*
- Mark Pollitt : "*information of probative value stored or transmitted in digital form*"
- Carrier: *"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence*
- A nexus between digital data, jurisprudence and science.

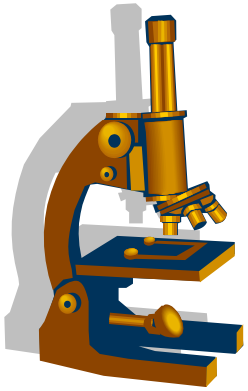
Development of High Quality Digital Forensics

- Digital forensics has mostly developed out of a demand for service (collection of electronic evidence) from the law enforcement community
  - in an ad hoc manner not a scientific one.
  - as a discipline that crosses the corporate, academic, scientific as well as the law enforcement domains
  - as a forensic science.
- Compliance with ISO 17025 standard for laboratory accreditation is becoming the main method of achieving the goal of establishing the quality required from a forensic science so as to provide robust evidence for the court.

Effect of Accreditation on Digital Forensic Process

- Accreditation brings structure and organization with procedures, documentation and testing.
- Implications
  - Establishment of investigative and technical processes
  - Standard Operating procedures
  - Validation and verification of test methods and processes.
- Problem
  - forensic tools are modified regularly in order to keep up with change in technology (the Cloud, android operating system, solid state technology?)
  - not all tools used by specialists were designed originally with the forensic process in mind, instead developed to meet the needs of particular interest groups, such as file system drivers, operating systems, Indexing engines,
  - Validation and verification in a dynamic environment

Current Forensic Environment in Other Disciplines



- The connotation of ‘forensic’ infers a scientific approach.
- In order for the discipline to adopt a scientific framework there needs to be scientific method and reproducibility of results
- ‘Need for speed’ from the increase in case load, from the increase in the amount of data requiring examination
- Trustworthiness of evidence is an issue
- Law enforcement has a way to go to meet minimum standards for a scientific discipline.
  - 58% of Agencies in the United States still did not have digital evidence policies
  - only 57% of agencies required specific training to duplicate, examine and analyze evidence and
  - more than 70% of Practitioners had no or minimal training in this discipline.

Existing digital evidence frameworks

- There are a number of frameworks and guidelines developed from academia and authoritative bodies, such as the Department of Justice and the Association of Chief Police Officers in the UK.
- None of these models specifically discusses the Cloud, extraction of robust evidence, and the accompanying accreditation which calls for the validation and verification of the tools and processes used to collect evidence.

Enter the Cloud!

- Cloud computing is a term used to describe the use of a collection of services, applications, data and infrastructure that can be rapidly orchestrated, provisioned and decommissioned (Mell & Grance 2009).
- Clouds achieve this by using innovative architectures in which resources are virtualised and resource management is largely automated.

Clouds provide an on-demand, cost-effective, elastically scalable utility-like model for meeting users' ICT requirements, in several different contexts.

Cloud Service and Deployment Models

- According to the US Government's National Institute of Standards and Technology (NIST) definition for computing (adopted by the Australian Government – see AGIMO 2011), cloud computing comprises three service models and four deployment models (Pell & Grance 2009).

Deployment models

- Private clouds provide resources for the sole use of a single enterprise, either to make better use of in-house resources, or as a model for managed delivery by an external service provider.
- Public clouds on the other hand are made available to multiple customers who can then purchase ICT as and when they need it, avoiding up-front investments and ongoing management costs.
- Community clouds are also possible, in which participants pool their ICT resources and manage them using cloud technology for some agreed purpose.
- (Hybrid models also exist in which multiple clouds (possibly of different types) are used to achieve the required characteristics.

Service models

- Cloud services can also be characterised according to the type of services they deliver to their users:
- Software-as-a-Service (SaaS) refers to complete applications provided to customers as fully or partially remote services;
- Platform-as-a-Service (PaaS), refers to the provision of a software platform upon which customers can build and deploy their own applications; and
- Infrastructure-as-a-Service (IaaS) refers to the provision of raw computing resources (virtualised servers and storage) for on-demand use by customers.

E-Crime and Cloud Computing

- Clouds present both challenges and opportunities for law enforcement and national security agencies, particularly digital forensic investigators.
- Clouds (like other networked cyber-infrastructure) are subject to frequent attacks by hackers, who may be able to hijack and use them for criminal purposes, so adding to the challenge of growing case volumes.

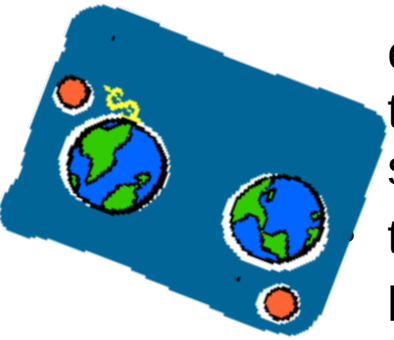
E-Crime and Cloud Computing

- In addition, cloud services can be used as a launching pad for new attacks or to store and distribute criminal data (e.g. child abuse materials for commercial purposes and terrorism-related materials) by cybercriminals, organised crime groups and politically-motivated actors to avoid the scrutiny of law enforcement and intelligence agencies (Choo 2010).

Possible Effect of Cloud based Cyber crime

- Use of cloud-based ICT by cybercriminals, organised crime groups and politically-motivated actors (or their victims) means that:
  - their devices will be virtualised, geographically distributed and ephemeral, presenting technical and jurisdictional challenges for their identification and seizure by law enforcement and national security agencies.

    this will impede digital forensic investigators and potentially prevent law enforcement and national security agencies from acquiring digital evidence and analysing digital content forensically in a timely fashion.
  - Will disrupt the continuity of businesses whose data and information are hosted on the seized hardware by law enforcement agencies – business continuity is one of the key risk areas identified by the Australian Government Information Management Office (AGIMO 2011).



Recognised Risks (AGIMO)

- Other risk areas associated with the use of cloud computing in Government identified by AGIMO (2011) include:
  - The dynamic nature of the cloud can result in confusion as to where information actually resides (or is transitioning through) at any given point in time, and impede **data/information retrieval** by forensic investigators.
  - Forensic investigators need to be aware of the **different legislative and regulatory requirements** in other jurisdictions as data/information is likely to be hosted in off-shore data centres.
  - **Skill requirements**: There will be an increasing demand for forensic investigators to be trained in data/information retrieval in the cloud computing environment.
- These risks provide business opportunities to the wise!

State of the Art in Research

- There is emerging research seeking to understand issues pertaining to the Cloud, E-Crime and Digital Forensics.
  - specific focus on issues surrounding legally seizing electronic devices in an investigation or where only partial data is required, across multiple locations, formats and jurisdictions (Lu et al 2010)
  - unresolved privacy issues associated with legally acquiring data held by third parties or from individual ‘clouds’ (Garfinkel & Cox 2009).
  - many who look at a number of additional security issues associated with data controlled by third party companies (Chow et al 2009).
  - no holistic investigative and technological framework for E-Crime, Digital forensics and the Cloud has been developed.

Possible Extensions for Cloud Forensics

- Aim is to provide a systematic approach allowing digital forensics to be used when criminals use clouds or other large virtualised cyber-infrastructure for storage or service or both.
  - Extend current models which allow for structured functional mapping of discipline so as to develop robust processes, validation and verification etc.
  - Developing investigative frameworks
  - Examining cloud remnants devices
  - Extend a Forensic Readiness Approach